UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,	)	
Plaintiff,	)	
	)	**Civil Case No. 10-1533 (RJL)**
v.	)	
NATIONAL SECURITY AGENCY,	)	
Defendant.	)	

MEMORANDUM OPINION
(July 8, 2011) [#9, #11]

Plaintiff Electronic Privacy Information Center ("EPIC" or "plaintiff") brings this action against the National Security Agency ("NSA" or "defendant") for failure to disclose information pursuant to the Freedom of Information Act ("FOIA"). Plaintiff seeks material relating to NSA's possible relationship with Google following news of an alleged cyber attack by hackers in China and of a subsequent cooperation agreement between Google and NSA. Before this Court is defendant's Motion for Summary Judgment and plaintiff's Cross-Motion for Summary Judgment. After due consideration of the parties' pleadings, the relevant law, and the entire record herein, defendant's motion is GRANTED and plaintiff's motion is DENIED.

BACKGROUND

On February 4, 2010, following media coverage of a possible partnership between the NSA and Google relating to an alleged cyber attack by hackers in China, EPIC submitted a FOIA request to NSA seeking:

1. All records concerning an agreement or similar basis for collaboration, final or draft, between the NSA and Google regarding cyber security;
2. All records of communication between the NSA and Google concerning Gmail, including but not limited to Google's decision to fail to routinely encrypt Gmail messages prior to January 13, 2010; and
3. All records of communications regarding the NSA's role in Google's decision regarding the failure to routinely deploy encryption for cloud-based computing service, such as Google Docs.

Compl. ¶ 12.

NSA denied EPIC's request. Letter from Pamela N. Phillips, NSA, FOIA/PA Office, Mar. 10, 2010 [#9-3]. While it acknowledged working "with a broad range of commercial partners and research associates," the Agency refused to "confirm [or] deny" whether it even had a relationship with Google. *Id.* In support of its response, NSA cited Exemption 3 of FOIA and Section 6 of the National Security Agency Act of 1959 ("NSA Act"), explaining that any response would improperly reveal information about NSA's functions and activities. *Id.* Such a response – neither confirming nor denying the existence of requested documents – is known as a *Glomar* response.[1]

On May 7, 2010, EPIC appealed through the agency's internal appeal process. Compl. ¶ 21. However, after NSA failed to respond to EPIC's appeal within the statutory deadline, EPIC filed the complaint initiating this lawsuit. Pl.'s Opp'n to Mot. For Summ.

[1] The term "*Glomar* response" is derived from the ship the *Glomar Explorer,* and refers to the C.I.A.'s refusal to acknowledge the existence or non-existence of any records pertaining to the ship. *Phillippi v. C.I.A.*, 546 F.2d 1009, 1011 (D.C. Cir. 1976).

J. at 3 (Pl.'s Opp'n).[2] On December 22, 2010, NSA filed its Motion for Summary Judgment, contending that the use of a *Glomar* response was appropriate under the circumstances and that the requested information was protected from release by FOIA Exemption 3, 5 U.S.C. § 552 (b)3, and Section 6 of the NSA Act, Sec. 6, Pub. L. No. 86-36, 73 Stat. 63, 50 U.S.C. § 402 note. Def.'s Mem. in Supp. of Mot. Summ. J. ("Def.'s Mot.") at 3.

In support of its motion, NSA submitted a declaration by Diane M. Janosek, the Deputy Associate Director for Policy and Records for the NSA ("Janosek Declaration" or "Declaration"). Decl. of Diane M. Janosek, Dec. 20, 2010 ("Janosek Decl.") [#9-1]. Specifically, the Declaration states that, as part of its Information Assurance mission, NSA is responsible for "protecting Department of Defense and other national-security information systems, as well as providing direct support to other agencies that help protect other U.S. government information systems and the nation's critical infrastructure and key resources." *Id.* ¶ 4. The NSA also performs government vulnerability discovery and security testing, and participates in public-private security initiatives relating to the commercial technology that the U.S. Government uses for its information systems. *Id.* ¶¶ 5-6.

With respect to EPIC's specific request, the Declaration states that "[t]o confirm or deny the existence of any such records would be to reveal whether the NSA . . . determined that vulnerabilities or cybersecurity issues pertaining to Google or certain of

[2] Once the suit was filed, NSA stopped processing EPIC's appeal and filed an answer on October 27, 2010 to EPIC's complaint. Def.'s Mot. at 4.

its commercial technologies could make U.S. government information systems susceptible to exploitation or attack." *Id.* ¶ 13. The Declaration further clarifies that even an acknowledgement of a relationship between the NSA and a commercial entity could potentially alert "adversaries to NSA priorities, threat assessment, or countermeasures," and that, as such, the information relates to the Agency's core functions and activities under its Information Assurance mission. *Id.* ¶¶ 13-14.

In response to NSA's Motion, EPIC filed a cross-motion on January 28, 2011. EPIC asserts two arguments: first, that NSA was required under FOIA to search for relevant records and segregate and disclose non-exempt information prior to issuing a *Glomar* response; and second, that the Janosek Declaration was "vague and conclusory," and, therefore, insufficient under the law of this Circuit. Pl.'s Opp'n at 4. For the following reasons, I disagree.

ANALYSIS

Summary judgment is appropriate when the record demonstrates that there is no genuine issue of material fact in dispute and that the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a). The moving party bears the burden, and the court will draw "all justifiable inferences" in favor of the non-moving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986). Nevertheless, the non-moving party "may not rest upon the mere allegations or denials of his pleading, but . . . must set forth specific facts showing that there is a genuine issue for trial." *Id.* at 248 (internal quotations omitted). Factual assertions in the moving party's affidavits may be accepted

as true unless the opposing party submits its own affidavits, declarations or documentary evidence to the contrary. *Neal v. Kelly*, 963 F.2d 453, 456 (D.C. Cir. 1992).

"When assessing a motion for summary judgment under FOIA, the Court shall determine the matter *de novo*." *Judicial Watch, Inc. v. U.S. Dep't of Homeland Sec.*, 598 F. Supp. 2d 93, 95 (D.D.C. 2009) (citing 5 U.S.C. § 552(a)(4)(B)). While the "burden is on the agency to sustain its action," 5 U.S.C § 552 (a)(4)(B), courts must give substantial weight to an agency's affidavits, *Hayden v. NSA/CSS*, 608 F.2d 1381, 1387 (D.C. Cir. 1979), *see Military Audit Project v. Casey*, 656 F.2d 724, 745 (D.C. Cir. 1981). The court may rely on the agency's affidavits or declarations if they contain reasonable specificity of detail rather than merely conclusory statements, and if they are not called into question by contradictory evidence in the record or by evidence of agency bad faith. *See Halperin v C.I.A.*, 629 F.2d 144, 150 (D.C. Cir. 1980). "Ultimately, an agency's justification for invoking a FOIA exemption is sufficient if it appears logical or plausible." *Larson v. U.S. Dep't of State*, 565 F.3d 857, 862 (D.C. Cir. 2009) (internal quotations omitted).

When an agency issues a *Glomar* response – refusing to confirm or deny the existence of documents – it must establish that the requested information is protected by one of the nine recognized FOIA exemptions. 5 U.S.C. § 552(b)(3); *see Wolf v. C.I.A.*, 473 F.3d 370, 375 (D.C. Cir. 2007). Exemption 3 permits an agency to prevent the release of records that are "specifically exempted from disclosure by statute." 5 U.S.C. § 552(b)(3). Although FOIA requests are traditionally "narrowly construed," *Dep't of the Air Force v. Rose*, 425 U.S. 352, 361 (1976), Exemption 3 "differs from other FOIA

exemptions in that its applicability depends less on the detailed factual contents of specific documents," *Goland v. C.I.A.*, 607 F. 2d 339, 350 (D.C. Cir. 1978). Instead, "the sole issue for decision is the existence of a relevant statute and the inclusion of withheld material within that statute's coverage." *Id.*; *see Ass'n of Retired R.R. Workers v. U.S. R.R. Ret. Bd.*, 830 F.2d 331, 336 (D.C. Cir. 1987).

It is well established that Section 6 of the NSA Act is a statutory exemption under Exemption 3. *See Hayden*, 608 F.2d at 1389; *Founding Church of Scientology of Washington, D. C., Inc. v. N.S.A.*, 610 F.2d 824, 826 (D.C. Cir. 1979). Section 6 of the NSA Act broadly prohibits the disclosure of information pertaining to the organization, function, or activities of the NSA. National Security Agency Act of 1959, Sec. 6, Pub. L. No. 86-36, 73 Stat. 63, 50 U.S.C. § 402 note. Specifically, the NSA need not disclose "the organization or any function of the National Security Agency, [or] any information with respect to the activities thereof." *Id.* While our Circuit has admonished that "courts must be particularly careful when scrutinizing claims of exemptions based on such expansive terms," as those included in Section 6, *Scientology*, 610 F.2d at 829, this heightened scrutiny must be tempered by the recognition of the substantial challenges posed to the NSA in maintaining operational security, *see Hayden*, 608 F.2d at 1390 (interpreting the NSA Act to reflect congressional recognition of the agency's "peculiar security needs").

Thus, once the agency, through affidavits, has created "as complete a public record as is possible" and explained "in as much detail as is possible the basis for its claim," *Phillippi*, 546 F.2d at 1013, the "court is not to conduct a detailed inquiry to

decide whether it agrees with the agency's opinions," *Halperin*, 629 F.2d at 148. Further, "NSA is not required to show harm to national security under Section 6." *Larson*, 565 F.3d at 868; *see also Hayden*, 608 F.2d at 1390. As the Supreme Court explained in *C.I.A. v. Sims*, "bits and pieces of data 'may aid in piecing together bits of other information even when the individual piece is not of obvious importance in itself.'" 471 U.S. 159, 178 (1985) (quoting *Halperin v. C.I.A.*, 629 F.2d 144, 150 (D.C. Cir. 1980)).

Here, NSA's supporting affidavits satisfy the criteria for non-disclosure under Section 6.[3] The Janosek Declaration contains sufficient detail, pursuant to Section 6, to support NSA's claim that the protected information pertains to "the organization or any function of the National Security Agency, [or] . . . to the activities thereof." 50 U.S.C. § 402 note; *see Hayden*, 608 F.2d at 1388 (granting summary judgment based on affidavits that describe "the activity involved, the need for maintaining secrecy, and the reason for believing that disclosure of any of the requested material could compromise legitimate secrecy needs"); *Miller v. Casey*, 730 F.2d 773, 776 (D.C. Cir. 1984) (describing as ample an affidavit which "demonstrates that the information withheld logically falls

[3] Plaintiff's argument regarding the public dissemination of information relating to a purported Google/NSA agreement is misleading. The agency has not waived its FOIA protections by official disclosure of the requested information. *See Wolf v. C.I.A.*, 473 F.3d 370, 378 (D.C. Cir. 2007). Nor does plaintiff ever contest this point. Rather, plaintiff incorrectly argues that information, which is widely reported in the media, is stripped of its FOIA protections. Pl.'s Opp'n at 9-10. Indeed, while *Glomar* responses are deemed inappropriate when the specific information has already been officially and publicly disclosed by the solicited agency, such disclosure "cannot be based on mere speculation, no matter how widespread." *Id.* The agency, itself, must waive FOIA protections through an official disclosure. *Id.*

within the claimed exemption, and [is] not controverted by either contrary evidence in the record nor by evidence of agency bad faith" (internal quotations omitted)).

Indeed, as the Janosek Declaration makes clear, the requested information relates to the NSA's cryptologic Information Assurance mission, which is designed to protect national security information systems and critical infrastructure resources. Janosek Decl. ¶ 5. Because of the reliance by the U.S. government on commercial systems, this mission includes the assessment of commercial technologies and the Agency's participation in public-private security initiatives. *Id.* ¶¶ 5-6, 12.

Thus, with respect to plaintiff's first request – all records concerning an agreement between NSA and Google regarding cyber-security – the Janosek Declaration explains that "any acknowledgement by NSA of the existence or nonexistence of a relationship or agreement with Google… would reveal whether or not NSA considered the alleged attack to be of consequence for critical U.S. government information systems." *Id.* ¶ 13. Further, with respect to plaintiff's second and third requests – NSA/Google communications regarding encryption of Gmail and cloud-based computing service, such as Google Docs – the Janosek Declaration clarifies that "to confirm or deny the existence of any such records would be to reveal whether NSA, in fulfilling one of its key missions, determined that vulnerability or cyber security issues pertaining to Google or certain of its commercial technologies could make U.S. government information systems susceptible to exploitation or attack by adversaries . . ." *Id.* ¶ 13. The Declaration then adds, "[i]n addition to revealing information about NSA functions and activities, such information falling in either category could alert our adversaries to NSA priorities, threat

assessments, or countermeasures that may or may not be employed against future attacks." *Id.*

This Declaration provides more than cursory details concerning the relationship between the withheld material and NSA's organization and function. *See Scientology*, 610 F.2d at 831. To the contrary, it explains the relevance of the Information Assurance mission to national security, the clear tie between the requested information and the Information Assurance mission, and the cognizable harm posed by acknowledging the existence/non-existence of the information.[4] Thus, because NSA's answer is both logical and plausible,[5] the Declaration satisfies all the requirements set forth by our Circuit. *See Larson*, 565 F.3d at 862; *Halperin*, 629 F.2d at 148; *Hayden,* 608 F.2d at 1388.

[4] EPIC argues that the NSA's single supporting declaration is conclusory and fails to demonstrate that the requested information pertains to the NSA's Information Assurance mission and is protected by the NSA Act exemption. Pl.'s Opp'n at 7-8. EPIC also challenges that its requests are broad enough to include documents that "do not reflect on the NSA's activities in any way." Pl.'s Opp'n at 6. These claims understate the Janosek Declaration's depiction of the NSA's Information Assurance mission, as well as the explanation of how the requested records would reveal information relating to NSA activities. Simply put, it is the relationship between Google and the NSA not just the content of records that warrants protections. *See Goland*, 607 F. 2d at 350.

[5] NSA also argues that revealing a relationship with Google could dissuade other companies from working with the agency in the future or self-reporting on problems. Def.'s Reply at 10. This is a serious concern which also warrants finding for the NSA. *See Sims,* 471 U.S. at 175.

CONCLUSION

For all of the foregoing reasons, the Court GRANTS defendant's Motion for Summary Judgment [#9] and DENIES plaintiff's Cross-Motion for Summary Judgment [#11]. An Order consistent with this decision accompanies this Memorandum Opinion.

RICHARD J. LEON
United States District Judge